Licenční smlouva

Smluvní strany

CYBOSEC s.r.o.
se sídlem: Hradčany 347, 503 53 Smidary,
zastoupená: Pavlem Jíchou, jako jednatelem společnosti,
IČO: 04301226,
DIČ: CZ04301226,
bankovní spojení: Fio banka, a. s.,
č. ú.: 2601103928/2010,
zapsaná v obchodním rejstříku vedeném Krajským soudem v Hradci Králové, oddíl C, vložka 42008
,
(dále jen „poskytovatel“)

a

město Sokolov
se sídlem: Rokycanova 1929, 356 01 Sokolov,
zastoupené: Renatou Oulehlovou, starostkou,
IČO: 00259586,
bankovní spojení: Komerční banka, a. s.,
č. ú.: 521391/0100,
(dále jen „nabyvatel“)

uzavírají níže uvedeného dne v souladu s příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, (dále jen „občanský zákoník“) tuto smlouvu:

Čl. 1
Úvodní ustanovení

Tato smlouva se uzavírá na základě výsledů zadávacího řízení na zadání veřejné zakázky malého rozsahu s názvem „Dodávka antivirového SW“ v souladu se zadávací dokumentací ze dne 12. 09. 2022 a nabídkou poskytovatele ze dne na plnění uvedené veřejné zakázky (dále jen „Nabídka“).

Čl. 2
Předmět smlouvy

2.1 Poskytovatel touto smlouvou a za podmínek v ní uvedených poskytuje nabyvateli právo užívat antivirový software Bitdefender GZ Business Security ENTERPRISE (ULTRA), jehož přesná specifikace je uvedena v Požadovaných technických parametrech produktu, jenž jsou přílohou č. 1 k této smlouvy, a v Nabídce, jenž je přílohou č. 2 k této smlouvě, (dále jen „antivirový SW“).

2.2 Součástí licenčního práva podle odst. 2.1 a odměny za něj jsou rovněž:
- a) právo na aktualizace virové databáze antivirového SW, programových komponent antivirového SW, právo upgradu na nové verze antivirového SW,
- b) poskytování servisní podpory antivirového SW,
- c) poskytování technické podpory antivirového SW v češtině v rozsahu 12/5 po telefonu, elektronickou poštou nebo vzdáleně, a to podle volby nabyvatele,
- d) instalace antivirového SW nebo provedení jeho aktualizace či upgrade v případě požadavku nabyvatele na jejich provedení, popř. pomoc s touto instalací či aktualizací,
- e) školení určených zaměstnanců nabyvatele stran užívání antivirového SW, konzultace, pomoc s instalací / nasazením / aktualizací / ověřením bezpečnostních politik v ceně.
- f) 4 hodiny práce poskytovatele související s předmětem smlouvy, provedené na vyžádání nabyvatele buď na místě (v sídle nabyvatele) nebo vzdáleně.

2.3 Práva podle odst. 2.1 a 2.2 se udělují jako nevýhradní na dobu uvedenou v čl. 4.

2.4 Právo podle odst. 2.1 se poskytuje v počtu 300 instalací na koncová zařízení, zahrnující stanice,

servery, mobilní zařízení a terminálové relace. Nabyvatel je oprávněn užívat antivirový SW na jakémkoliv zařízení v jeho vlastnictví, avšak v maximálním počtu licencí podle věty první, s tím, že licenci podle této smlouvy není povinen využít.

2.5 Poskytovatel je oprávněn k výkonu práva, ke kterému udělil nevýhradní licenci podle této smlouvy, jakož i poskytnout licenci podle této smlouvy nabyvateli.

2.6 Poskytovatel garantuje, že antivirový SW má vlastnosti uvedené v Nabídce a v příloze č. 1 - Požadované technické parametry produktu.

Čl. 3
Odměna

3.1 Odměna za užívání licence za celou dobu trvání smlouvy podle čl. 4 se sjednává ve výši 419.622,00 Kč (slovy: čtyřistadevatenácttisícšestsetdvacetdvěkorunyčeské) bez DPH. K odměně se připočte DPH v příslušné zákonné sazbě.

3.2 Odměna podle předchozího odstavce zahrnuje odměnu za práva k užívání antivirového SW v rozsahu podle této smlouvy včetně jeho aktualizace, upgrade a poskytování servisní a technické podpory.

3.3 Odměna podle odst. 3.1 je konečná, nejvýše přípustná a pevná a zahrnuje veškeré náklady poskytovatele spojené s poskytováním plnění podle této smlouvy včetně odměny za poskytnutí licence k užívání dodaného softwaru. Jediným důvodem změny výše odměny je změna zákonné sazby DPH.

3.4 Odměna podle odst. 3.1 je splatná ve třech rovnoměrných částech za každý rok trvání smlouvy, a to na základě daňového dokladu (faktury) vystaveného poskytovatelem. Fakturu na úhradu části odměny za první rok trvání smlouvy vystaví poskytovatel do 14 dnů od předání antivirového SW podle čl. 4 odst. 4.2. Faktury na úhradu části odměny za druhý a následující roky trvání smlouvy vystaví poskytovatel vždy do 14 dnů od počátku příslušného roku, za který se má odměna hradit.

3.5 Faktura musí obsahovat veškeré náležitosti daňového dokladu stanovené příslušnými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Nebude-li faktura splňovat veškeré náležitosti řádného daňového dokladu nebo bude-li mít jiné závady v obsahu, je nabyvatel oprávněn ji ve lhůtě její splatnosti poskytovateli vrátit a ten je povinen vystavit fakturu opravenou či doplněnou. V případě vrácení faktury poskytovateli se lhůta splatnosti přerušuje a nová lhůta splatnosti počíná běžet od počátku dnem následujícím po dni, kdy byla opravená či doplněná faktura splňující všechny náležitosti doručena nabyvateli.

3.6 Odměna je splatná do 30 dnů od ode dne doručení faktury nabyvateli, a to bezhotovostním převodem na bankovní účet poskytovatele uvedený v záhlaví této smlouvy.

3.7 Za den úhrady odměny se považuje den odepsání fakturované částky z účtu nabyvatele ve prospěch účtu poskytovatele.

3.8 Poskytovatel nemá nárok na zaplacení části odměny za dobu, po kterou nebyl antivirový SW dostupný či poskytován.

Čl. 4
Doba trvání licence a dodací podmínky

4.1 Závazek zřízený touto smlouvou se sjednává na dobu určitou v trvání 3 let počínaje dnem účinnosti této smlouvy.

4.2 Poskytovatel předá nabyvateli antivirový SW formou předání příslušných licenčních klíčů elektronickou poštou na adresu [redacted] a to bezodkladně, nejpozději však do 5 dnů od nabytí účinnosti této smlouvy. Spolu s antivirovým SW předá poskytovatel nabyvateli veškeré doklady potřebné k řádnému užívání antivirového SW v českém jazyce.

4.3 Instalaci antivirového SW jakož i aktualizace a upgrade podle čl. 2 odst. 2.2 písm. a) provádí nabyvatel svépomocí, přičemž má právo k tomu využít podporu poskytovatele podle čl. 2 odst. 2.2 písm. d) a ten je povinen mu ji bezodkladně poskytnout.

Čl. 5
Ukončení smlouvy

5.1 Každá ze smluvních stran je oprávněna tuto smlouvu vypovědět bez udání důvodu s 6měsíční výpovědní dobou počínající běžet prvního dne následujícího po jejím doručení.

5.2 Nabyvatel je kromě důvodů pro odstoupení od smlouvy stanovených občanským zákoníkem oprávněn odstoupit od této smlouvy v případě, že:

a) poskytovatel je v prodlení s dodáním antivirového SW podle čl. 4 odst. 4.2 déle než 10 dnů,
b) antivirová ochrana prostřednictvím antivirového SW bude nedostupná déle než 24 hodin po sobě jdoucích,
c) proti poskytovateli bude zahájeno insolvenční řízení a insolvenční návrh nebude v zákonné lhůtě odmítnut pro zjevnou bezdůvodnost nebo insolvenční návrh prodávajícího bude zamítnut proto, že majetek prodávajícího nepostačuje ani k úhradě nákladů insolvenčního řízení, anebo prodávající vstoupí do likvidace,
d) ukáže-li se prohlášení poskytovatele podle čl. 2 odst. 2.5 nebo 2.6 nepravdivým.

5.3 Poskytovatel je oprávněn odstoupit od smlouvy v případě prodlení nabyvatele s úhradou odměny podle čl. 3 delšího než 30 dní.

5.4 Účinky odstoupení nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

5.5 Odstoupením od smlouvy není dotčen nárok na smluvní pokutu ani na náhradu škody.

Čl. 6
Smluvní pokuty

6.1 V případě prodlení s dodáním antivirového SW podle čl. 4 odst. 4.2 je poskytovatel povinen zaplatit nabyvateli smluvní pokutu ve výši 1 000 Kč za každý i započatý den prodlení.

6.2 V případě nedostupnosti aktualizačních serverů pro aktualizaci antivirového SW je poskytovatel povinen uhradit nabyvateli smluvní pokutu, jejíž výše se určí jako procentní část roční části odměny podle čl. 3 odst. 3.4 takto:

Měsíční dostupnost antivirového SW	**Smluvní pokuta**
Dostupnost nižší než 100 % - 99,0 % vč.	5 %
Dostupnost nižší než 99,0 % - 97,0 % vč.	10 %
Dostupnost nižší než 97,0 %	20 %

6.3 Nabyvatel je oprávněn požadovat po poskytovateli zaplacení smluvní pokuty ve výši 500 Kč v případě porušení jakékoliv jiné povinnosti uvedené v této smlouvě za každý den prodlení s nápravou přes výzvu nabyvatele o více než 3 dny po doručení takovéto výzvy.

6.4 Úhradou smluvní pokuty není dotčeno právo na náhradu škody způsobené porušením povinnosti, pro kterou je smluvní pokuta sjednána.

6.5 Smluvní pokuta je splatná na základě písemné výzvy nabyvatele do 15 dnů od doručení výzvy poskytovateli převodem na účet uvedený v záhlaví této smlouvy.

6.6 Povinnost zaplatit smluvní pokutu může vzniknout i opakovaně a její celková výše není omezena.

6.7 Povinnost zaplatit smluvní pokutu trvá i po skončení této smlouvy či odstoupení od ní.

6.8 Poskytovatel považuje smluvní pokuty sjednané v tomto článku za přiměřené a vzdává se práva domáhat se u soudu jejich snížení.

6.9 Nabyvatel je oprávněn jakoukoliv smluvní pokutu podle této smlouvy jednostranně započítat proti jakékoli pohledávce poskytovatele za nabyvatelem, včetně pohledávky poskytovatele na zaplacení odměny podle čl. 3.

Čl. 7
Odpovědnost za škodu

7.1 Odpovědnost za škodu se řídí ust. § 2894 a násl. občanského zákoníku. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k jejich minimalizaci.

7.2 Poskytovatel neodpovídá za újmy, které by mohly vzniknout v souvislosti s užíváním předmětu této licenční smlouvy.

7.3 Poskytovatel je povinen za nabyvatele úplně a bez jeho přispění vyřídit a urovnat jakékoli požadavky třetích osob vyplývající z případných autorských práv (jejich možného porušení, atp.) k předmětu smlouvy.

Čl. 8
Závěrečná ustanovení

8.1 V případě neplatnosti některého ustanovení této smlouvy nebo v případě, že se některé ustanovení této smlouvy stane neplatným později, nemá tato skutečnost vliv na platnost této smlouvy jako celku.

8.2 Tato smlouva může být změněna pouze písemnou dohodou obou smluvních stran formou vzestupně číslovaných dodatků.

8.3 Právní vztahy touto smlouvou neupravené se řídí ustanoveními občanského zákoníku.

8.4 Veškeré písemnosti si budou strany této smlouvy předávat osobně, zasílat na adresy uvedené v záhlaví této smlouvy nebo do datové schránky, nestanoví-li se v této smlouvě jinak. Pro vztahy z této smlouvy se písemnost zaslaná doporučeně prostřednictvím České pošty, s. p., bude považovat za doručenou i v případě, že se z jakéhokoliv důvodu vrátí taková zásilka zaslaná na adresu v záhlaví této smlouvy jako nedoručená, a to i v případě, že se na této adrese nebude smluvní strana zdržovat.

8.5 Tato smlouva se vyhotovuje ve 2 stejnopisech, z nichž každá strana smlouvy obdrží po jednom stejnopisu.

8.6 Strany této smlouvy prohlašují, že tuto smlouvu uzavřely svobodně a vážně a pokládají ji za určitou a srozumitelnou. Po jejím přečtení prohlašují, že s jejím zněním souhlasí, což stvrzují svými podpisy.

8.7 Smlouva nabývá platnosti dnem podpisu obou smluvních stran a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Smluvní strany se dohodly, že smlouvu bez zbytečného odkladu uveřejní podle předchozí věty nabyvatel. Nabyvatel se zavazuje vyrozumět poskytovatele o uveřejnění smlouvy prostřednictvím registru smluv bez zbytečného odkladu poté, kdy sám obdrží potvrzení o uveřejnění smlouvy.

8.8 Smluvní strany výslovně prohlašují, že žádné ustanovení této smlouvy není obchodním tajemstvím podle § 504 občanského zákoníku ani neobsahuje důvěrnou informaci o poměrech smluvní strany nebo skutečnostech, které má smluvní strana potřebu ochraňovat jako důvěrnou informaci nebo předmět obchodního tajemství.

8.9 Nedílnou součástí smlouvy jsou následující přílohy:

a) Příloha č. 1 – Požadované technické parametry produktu
b) Příloha č. 2 – Nabídka poskytovatele

V Sokolově

Za nabyvatele:

……..
Renata Oulehlová, starosta/ka

V Praze

Za poskytovatele:

……..
Pavel Jícha, jednatel

Příloha č. 1 - Požadované technické parametry produktu:

Uchazeč kromě Ano/Ne uvede také popis řešení daného požadavku nebo obchodní název technologie, kterou je požadovaná funkcionalita zajištěná.

1. ZÁKLADNÍ POŽADAVKY NA SYSTÉM	
1.1. Prevence proti útokům	
a) Rezidentní real -time ochrana proti známým škodlivým kódům, tj. zejména, ale nejen: viry, červy, malware, rootkity, trojské koně, spyware, addware, phishing, keyloggery, postinfekční i další neznámé hrozby;	ANO
b) Integrovaný firewall (dále také „FW“) s možností centrální správy a definic politik, a to minimálně v rozsahu: – zdrojová IP adresa(subnet); – cílová IP adresa (subnet); – číslo (rozsah) TCP a UDP portů; – akce povolit/zakázat; – možnost logovat pravidlo;	ANO
c) Ochrana proti Ransomware - automatická reakce systému na počátek pokusu o šifrování souborů a zahájení automatických akci vedoucích k obnově původních souborů;	ANO
d) Nabízené řešení bude obsahovat vlastní systém pro hlídání a vytváření záloh souborů – obnova pouze s pomocí funkce Shadow Copy není přípustná;	ANO
e) Schopnost aktualizace nejen obsahu (virové definice, signatury), ale i vlastního kódu programového vybavení na koncovém zařízení, na nové verze s využitím automatické aktualizace;	ANO
1.2. Požadavky na vícevrstvou ochranu	
a) Ochrana proti 0-day útokům v preventivním režimu, včetně prvního výskytu 0-day malwaru;	ANO
b) Ochrana proti 0-day útokům ransomware;	ANO
c) URL filtering s plnou HTTPS visibilitou bez použití HTTPS inspekce, včetně kategorizace URL dle obsahu/zaměření, s možností zákazu nebo logování přístupu určité kategorie;	ANO
d) Ochrana proti phishingu zahrnující 0-day ochranu, včetně neznámých variant phishingových kampaní;	ANO
e) Ochrana proti zapojení koncového zařízení do sítě botnet (C&C);	ANO
f) Možnost do budoucna rozšířit nabízené řešení o centrální, administrátorem spravovatelné zabezpečení proti zranitelnostem pro fyzické a virtuální servery, Golden image, pracovní stanice Windows a aplikace třetích stran.	ANO
g) Nabízené řešení musí obsahovat subsystém proaktivní, heuristické a behaviorální analýzy chování aplikací a systémů;	ANO
h) Ochrana prověřováním externích medií, např. USB disk;	ANO
i) Blokace periferních zařízení (USB tiskárny, Bluetooth, Kameera) s podporou white listu na základě definice výrobce, modelu nebo sériového čísla.	ANO
j) Ochrana přístupu k infikovaným webovým stránkám;	ANO
1.3. Dodané řešení musí minimálně podporovat:	
a) Plánování automatického prověřování na hrozby;	ANO
b) Možnost specifikovat, zda prověřovat i vyměnitelná média a síťové disky;	ANO
c) Náhodné spuštění úloh prověření v náhodných intervalech;	ANO

d) Vynucení vzdáleného spuštění prověření na koncovém zařízení bez interakce uživatele;	ANO
a) Vynucení okamžité aktualizace databáze známých hrozeb nebo programového vybavení na vybraných zařízeních;	ANO
e) Možnost aktualizace koncového zařízení bez nutnosti připojení k síti objednatele;	ANO
f) Sběr informací o virových nákazách a hrozbách z koncových zařízení, logy skenování;	ANO
g) Koncový uživatel musí mít možnost volby odložit instalaci aktualizace programového vybavení na koncovém zařízení, přičemž doba odkladu musí být konfigurovatelná administrátorem systému;	ANO
h) Rychlé základní prověření na hrozby na libovolném koncovém zařízení;	ANO
i) Přístup do historie prověřování na hrozby koncových zařízení;	ANO
j) Možnost nastavení typů prověřovaných souborů;	ANO
k) U firewallu požadována možnost odpojit koncové zařízení od sítě (uvalení karantény);	ANO
l) Schopnost on-line komunikace programového vybavení s centrální databází výrobce pro detekci neznámých hrozeb, které ještě nejsou součástí lokální databáze na koncovém zařízení;	ANO
m) Možnost nastavení více aktualizačních serverů na koncovém zařízení podle síťového prostředí: – v síti objednatele; n) při přímém připojení na Internet;	ANO
2. POŽADAVKY NA SPRÁVU SYSTÉMU	
2.1. Správa řešení:	
a) Centrální správa koncových zařízení musí být řešena formou „Cloud management console“ (CMC) výrobce, instalace on-premise serveru v ICT prostředí objednatele není přípustná;	ANO
b) CMC musí umožňovat kompletní management celého řešení, všech koncových zařízení a všech funkcionalit, bez nutnosti instalace jakýchkoli dalších podpůrných prostředků, vyjma aktualizačních serverů v ICT prostředí objednatele;	ANO
c) CMC musí podporovat možnost rozdělení koncových zařízení do minimálně 3 samostatných, navzájem oddělených managementů;	ANO
d) CMC musí podporovat škálovatelnost úrovní přístupů – definování profilů;	ANO
e) CMC musí umožnit seskupování koncových zařízení do skupin dle požadovaného stupně chování a import seznamu koncových zařízení do těchto skupin;	ANO
f) CMC musí umožňovat nastavení různých zón firewallu;	ANO
g) CNC musí umožňovat správu koncových zařízení, které jsou mimo síť objednatele a nemají VPN připojení;	ANO
h) CNC musí umožňovat průběžné navyšování/snižování počtu koncových zařízení bez nutnosti opravy/reinstalace/rekonfigurace CNC;	ANO
i) Možnost centralizované i decentralizované správy včetně: – deploymentu programového vybavení na koncová zařízení (volitelně s možností použití Active Directory); – automatické distribuce nových verzí programového vybavení; – editace nastavení parametrů programového vybavení na koncovém zařízení; – vzdálená instalace na více koncových zařízení současně;	ANO

2.2. Centrální reporting	
a) Funkce automatického vytváření forenzních reportů z detekovaných incidentů, obsahujících kompletní průběh útoku, včetně možnosti stažení reportů uživatelem i administrátorem;	ANO
b) Centrální monitor událostí s možností detailního filtrování; možnost vytváření vlastních reportů nebo využití předefinovaných reportů;	ANO
c) EDR funkcionalita pro analýzu incidentů, včetně kategorizace útoků dle matice MITRE ATT&CK;	ANO
d) Sběr dat musí probíhat kontinuálně po celou dobu běhu agenta bez nutnosti spouštět tuto úlohu na koncovém zařízení manuálně nebo v reakci na incident;	ANO
3. IMPLEMENTAČNÍ OMEZENÍ	
3.1. Požadovaná podpora platforem operačních systémů:	
a) Pro koncová zařízení typu PC desktop a notebook jsou to Windows 8.1, Windows 10 a Windows 11, ve 32-bit i 64-bit verzi operačního systému (Windows 11 pouze 64-bit), včetně virtuálních PC se stejným OS provozovaných na platformě VMware Horizon;	ANO
b) Pro koncová zařízení s macOS verze 10.14 a vyšší;	ANO
c) Pro koncová zařízení s OS Windows Server 2012R2, 64-bit a všech následujících verzí (včetně clusteru); včetně virtuálních serverů na platformě VMware;	ANO
d) Pro koncová zařízení s OS Linux – minimálně v edicích RedHat 7.8, Debian 9.12, CentOS 7.8, Ubuntu 16,04, Oracle Linux 7.9, vše ve verzi 64-bit a všech následujících verzích;	ANO
e) Licenční model musí umožnit licencovat fyzické i virtuálních koncová zařízení;	ANO
f) Možnost rozšíření a podpory nabízeného řešení o ochranu mobilních zařízení;	ANO
4. ROZŠÍŘENÉ POŽADAVKY NA SYSTÉM OCHRANY	
a) Řešení pro koncová zařízení musí být v českém jazyce; včetně konzole správy, klientské aplikace a manuálů	ANO
b) Výrobce nesměl získat na av-comparatives (https://www.av-comparatives.org/awards/) za poslední 2 roky ani jednou méně než 3 hvězdy v kategorii „Real World Protection“ u firemních řešení.	ANO
c) Zastavení, vypnutí nebo odinstalace EDR systému a jeho komponent na koncovém zařízení musí být chráněno minimálně heslem;	ANO
d) Jakákoliv modifikace EDR systému a jeho komponent na koncovém zařízení musí být chráněna minimálně heslem;	ANO
e) Technologie Sandbox, CDR, EDR a Cloud Management Console jsou požadovány jako součást dodaného řešení;	ANO

Provozní
Požadované počty licencí

Zadavatel požaduje dodání licencí pro:

- 300 ks rezidentů na koncových zařízeních (stanice, servery, mobilní zařízení a terminálové relace)

Dodavatel navrhne optimální způsob licencování s ohledem na rozdílný počet uživatelů a zařízení.

Zadavatel požaduje dodávku výše uvedených licencí na dobu 3 let včetně podpory. Platby se předpokládají v následujícím režimu:

1. rok bude zaplacena cena za licence a za podporu na první rok
2. rok bude zaplacena cena za prodloužení podpory o další rok
3. rok bude zaplacena cena za prodloužení podpory o další rok

Součástí instalace školení, konzultace, pomoc s instalací / nasazením / aktualizací / ověřením bezpečnostních politik v ceně.
Dále pak možnost vyžádat jednou ročně, 4 hodiny práce na místě/vzdáleně tíž v ceně dodávky.

▪ Technická podpora v češtině.
▪ Technická podpora zdarma 12/5 poskytující pomoc na telefonu / přes e-mail / vzdáleně.

Bitdefender
GravityZone

Nabídka pro Město Sokolov

Sokolov CYBOSEC We build the Trust

Bitdefender®
BUILT FOR RESILIENCE

Společnost **Bitdefender je lídrem v oblasti kybernetické bezpečnosti**, který poskytuje nejlepší řešení prevence, detekce a reakce na hrozby ve své třídě po celém světě. Celosvětově chrání více jak 500 000 000 strojů ve 150 zemích. Pomocí mnohavrstvé ochrany s využitím strojového učení a umělé inteligence umí odhalovat a zablokovat i ty nejsofistikovanější útoky (Ransomware, bez souborové, cílené atd.).

Bitdefender
GravityZone

PRAVIDELNĚ VÍTĚZÍ V TESTECH

AV-TEST, 4 ocenění v roce 2020

FORRESTER®
WAVE LEADER 2019
Cloud Workload Security

Lídr v prvním hodnocení Forrester® WAVE™ pro zabezpečení cloudové pracovní zátěže

AV comparatives
Real-World Protection 2021
GOLD

Nejvíce umístění na 1. místě v letech 2018 až 2022 ve srovnávacích testech AV Comparatives

MITRE | ATT&CK®

Nejvyšší celkový počet detekcí a 100% detekce útočných technik pro Linux v hodnocení MITRE ATT&CK® 2021

FORRESTER®

"Největší dodavatel EDR, o kterém jste neuvažovali, ale měli byste", The Forrester® Wave™:

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Největší hráč v oblasti Radicati Endpoint Security MQ 2020

GravityZone ENTERPRISE (ULTRA)

Dokonalé řešení pro ochranu koncových bodů: pokročilá prevence, rozšířená detekce, účinná reakce a analýza rizik. Velmi výkonný EDR nástroj.
GravityZone Ultra kombinuje nejúčinnější ochranu na světě s funkcemi eXtended Endpoint Detection and Response (XEDR), které vám pomohou chránit vaši infrastrukturu koncových bodů (pracovních stanic, serverů nebo kontejnerů) v celém životním cyklu hrozeb, a to s vysokou účinností a efektivitou.

Nová korelace událostí napříč koncovými body posouvá detekci a sledování hrozeb na novou úroveň tím, že kombinuje granularitu a bohatý bezpečnostní kontext EDR s analýzou celé infrastruktury XDR (eXtended Detection and Response).

Díky zabudované analýze rizik (pro rizika generovaná koncovým bodem a uživateli) a inovacím v oblasti hardeningu, nativně minimalizujeme útočný povrch koncového bodu, čímž útočníkům ztěžujeme průnik.

S řešením GravityZone Ultra zkrátíte dobu potřebnou k odhalení hrozeb a reakci na ně prostřednictvím integrovaného bezpečnostního systému, a zároveň snížíte potřebu řešení od více dodavatelů.

Jak GravityZone ENTERPRISE (Ultra) pomáhá?

Nejúčinnější ochrana koncových bodů na světě

GravityZone sjednocuje technologie EDR, analýzy rizik a hardeningu v jednom jediném agentovi a jedné konzoli a využívá 30 vrstev pokročilých technik k úspěšnému zastavení narušení v celém životním cyklu hrozeb, od prvního kontaktu, zneužití, setrvání a škodlivé aktivity.

eXtended Endpoint Detection and Response (XEDR)

Nová funkce detekce a reakce na koncové body rozšiřuje možnosti analýzy EDR a korelace událostí za hranice jednoho koncového bodu, aby vám pomohla efektivněji řešit komplexní kybernetické útoky zahrnující více koncových bodů. XEDR vám jedinečným způsobem poskytuje vizualizace hrozeb na úrovni organizace, abyste se mohli zaměřit na vyšetřování a efektivněji reagovat.

Zabezpečení koncového bodu a člověka na základě analýzy rizik

Bitdefender engine pro analýzu rizik vám umožňuje průběžně vyhodnocovat, upřednostňovat a zpřísňovat chybné konfigurace a nastavení zabezpečení koncových bodů pomocí přehledného seznamu priorit. Identifikuje také akce a chování uživatelů, které představují bezpečnostní riziko pro vaši organizaci.

Zjednodušením a automatizací bezpečnostních operací, a neustálým zmenšováním plochy útoku, dosáhnete nejvyšší úrovně ochrany s nejnižšími náklady na provoz.

Nejúčinnější ochrana koncových bodů na světě

Výsledkem špičkové ochrany, kterou v současné době licencuje více než 150 předních technologických společností, je více než 30 technologií ochrany vyvinutých za posledních 20 let špičkovými výzkumníky, matematiky a datovými vědci společnosti Bitdefender. Kvalitu Bitdefenderu potvrzují i výsledky nezávislých testů, kdy např. v letech 2018 až 2021 získal Bitdefender většinu 1. míst ve srovnávacích testech AV.

Lokální a cloudové strojové učení

Bitdefender poprvé spustil strojové učení v roce 2009, což vedlo ke zvýšení detekce hrozeb s nízkým počtem falešně pozitivních výsledků, které mohou zastavit neznámé hrozby před jejich spuštěním a při jejich spuštění.

Hyperdetect - nastavitelné strojové učení

Umožňuje týmům IT vyladit ochranu citlivých podnikových služeb s nejvyšším rizikem.

Obrana proti anomáliím

Pokročilá technologie strojového učení, která sleduje systémové služby a monitoruje techniky skrytých útoků. Dokáže chránit vlastní aplikace před škodlivými útoky.

Cloudový Sandbox

Zajišťuje předběžnou detekci pokročilých útoků automatickým odesíláním souborů, které vyžadují další analýzu, do cloudového sandboxu, a přijímáním nápravných opatření na základě výsledku šetření.

Obrana proti síťovým útokům

Detekce a blokování nových typů hrozeb v dřívějších fázích útočného řetězce, jako jsou útoky hrubou silou, krádeže hesel a postranní pohyb.

Exploit Defense

Několik mechanismů pro prevenci zneužití chrání paměť a blokuje útoky před zneužitím systémů, což snižuje nároky na zpracování.

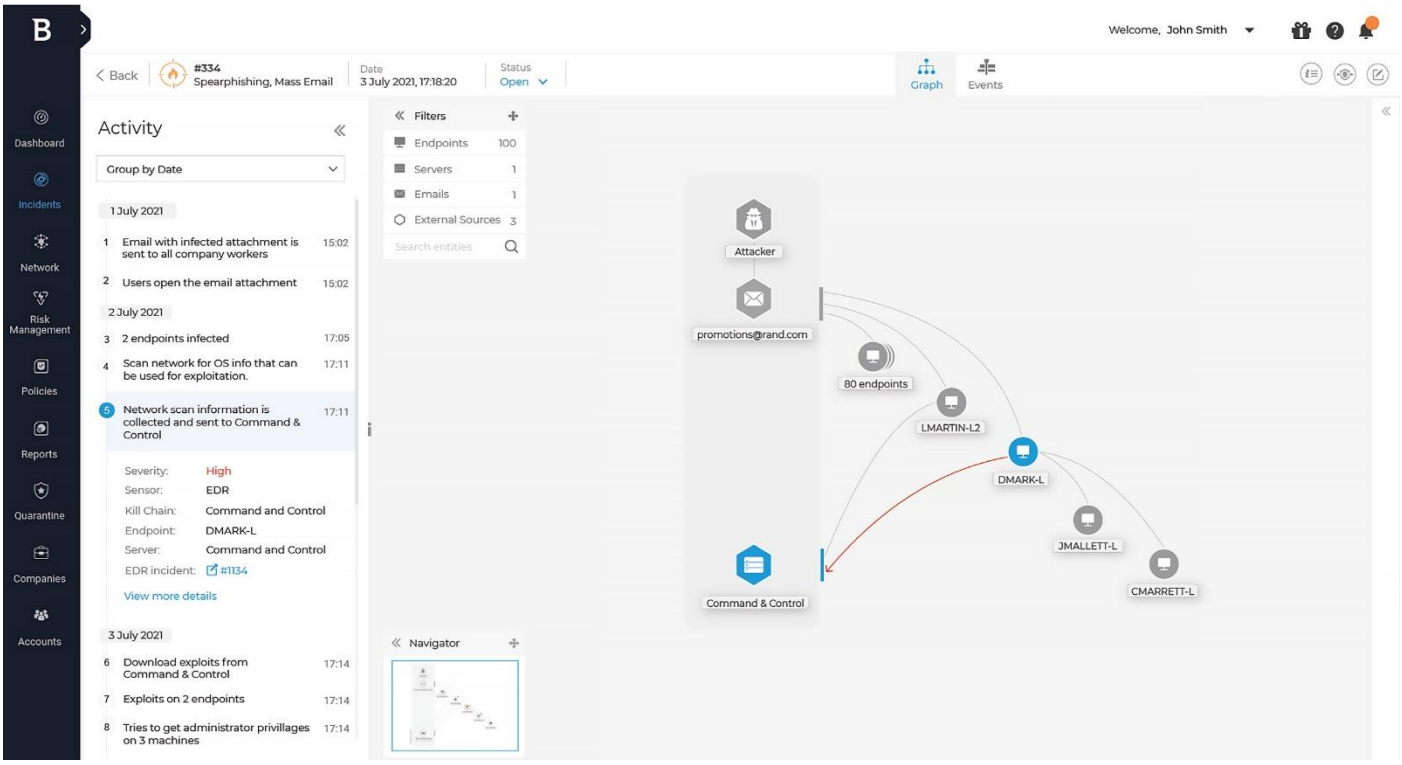
Obrana před bez souborovým útokem

Detekce a blokování malwaru založeného na skriptech, bez souborů, obfuskovaného a vlastního malwaru s automatickou nápravou.

Rozšířené vyšetřování incidentů a inteligentní reakce pro rozvinuté systémy

GravityZone Ultra umožňuje efektivní vyšetřování incidentů a rychlou reakci pro obnovení koncových bodů do stavu "lepšího než předtím". Nástroje pro vyšetřování incidentů, jako je Extended Incident View, poskytují přehled o bezpečnostních incidentech na úrovni organizace a pomáhají bezpečnostním týmům ověřovat podezřelé aktivity a adekvátně reagovat na kybernetické hrozby. Pokročilé vyhledávání aktuálních a historických dat na základě IOC, značek MITRE a dalších relevantních artefaktů, umožňuje rychlou identifikaci hrozeb, které se mohou skrývat v infrastruktuře koncových bodů.

Na základě informací získaných z koncových bodů během vyšetřování poskytuje jednotné rozhraní pro řízení nástrojů pro okamžitou úpravu zásad a/nebo záplatování zjištěných zranitelností, aby se předešlo budoucím incidentům a zlepšilo se zabezpečení prostředí.



Rozšířený pohled na incident poskytuje přehled o incidentu na úrovni organizace. Bezpečnostní analytik může snadno získat podpůrné důkazy a účinně reagovat. Analýza rizik koncových bodů pro nepřetržitou správu útočné plochy

Klíčové vlastnosti

eXtended Endpoint Detection and Response (XEDR)
Tato technologie korelace napříč koncovými body, známá jako eXtended EDR, posouvá detekci hrozeb a jejich viditelnost na novou úroveň tím, že využívá funkce XDR pro detekci pokročilých útoků napříč více koncovými body v hybridních infrastrukturách (pracovní stanice, servery nebo kontejnery s různými OS).

Integrovaná analýza lidských rizik a rizik koncového bodu
Průběžně analyzujte rizika pomocí stovek faktorů, abyste odhalili a upřednostnili konfigurační rizika pro všechny koncové body a umožnili automatické akce na jejich posílení. Identifikuje akce a chování uživatelů, které představují bezpečnostní riziko pro organizaci, jako je používání nešifrovaných webových stránek pro přihlašování na webové stránky, špatná správa hesel, používání kompromitovaných USB, opakované infekce atd.

Vrstvená obrana
Technologie bez signatur, včetně pokročilého lokálního a cloudového strojového učení, technologie analýzy chování, integrovaného sandboxu a vytvrzení (hardening) zařízení, fungují jako vysoce účinná vrstvená ochrana proti sofistikovaným hrozbám.
Integrovaná analýza lidských rizik a rizik koncového bodu

Vyšetřování a reakce na incidenty s nízkými náklady
Rychlé třídění upozornění a vyšetřování incidentů pomocí časové osy útoku a výstupu ze sandboxu umožňuje týmům pro reakci na incidenty rychle reagovat a zastavit probíhající útoky (reakce na jedno kliknutí).

Moderní prevence a detekce nové generace s automatickou nápravou
Nejlepší prevence na světě a funkce detekce, založené na chování při spuštění, zabraňují spuštění pokročilých hrozeb v podnikové infrastruktuře a zastavují je. Díky pokročilým funkcím prevence, jako jsou PowerShell Defense, Exploit Defense a Anomaly Detection, blokuje GravityZone Ultra moderní útoky v dřívějších fázích útočného řetězce, v době před jejich provedením, čímž zajišťuje neprůstřelnost zabezpečení vaší organizace. Po zjištění aktivní hrozby se spustí automatická reakce pro zablokování dalšího poškození nebo postranních pohybů.

Ochrana proti síťovým útokům
Bitdefeder Network Attack Defense, nová vrstva zabezpečení koncového bodu sítě navržená tak, aby detekovala a zabránila pokusům o útok, které využívají síťové zranitelnosti, blokuje několik síťových útoků založených na datovém toku, jako je Brute Force, Password Stealers nebo Lateral Movement, ještě předtím, než se mohou spustit. Network Attack Defense také generuje incidenty EDR a je důležitým zdrojem informací pro korelace incidentů EDR.

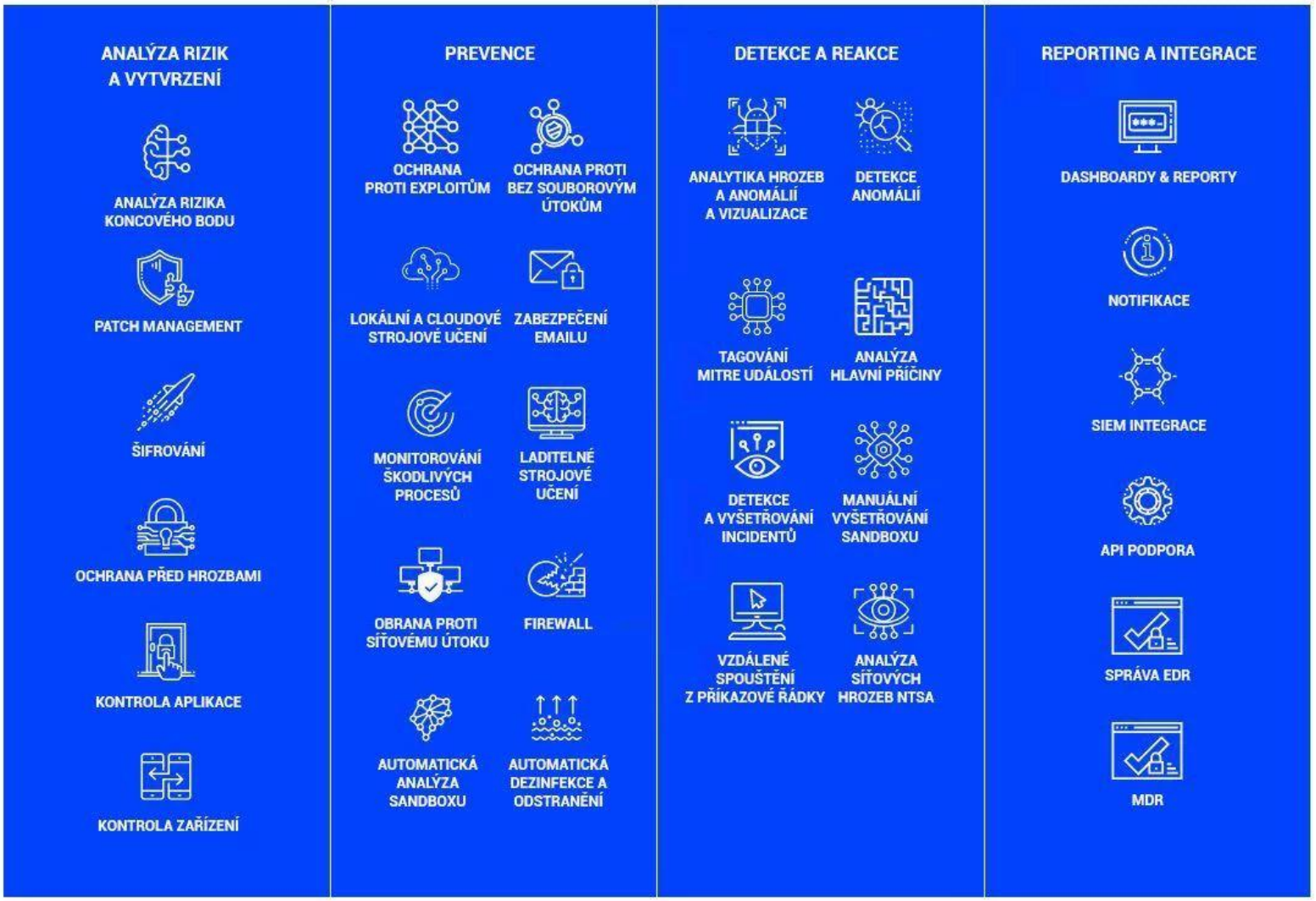
Pokrytí napříč platformami a integrace API třetích stran
Pokrývá všechny podnikové koncové body se systémem Windows, Linux nebo Mac ve fyzické, virtualizované nebo cloudové infrastruktuře, a poskytuje konzistentní zabezpečení napříč celou

infrastrukturou. Podporuje integraci s již existujícími nástroji pro bezpečnostní operace (včetně Splunku) a je optimalizován pro technologie datových center včetně všech hlavních hypervizorů.

Technologie GravityZone ENTERPRISE (Ultra)

Vytvořeno pro zvýšení kybernetické odolnosti

Bitdefender GravityZone Ultra spoléhá na architekturu jednoho agenta/jedné konzole, která poskytuje kompletní sadu bezpečnostních funkcí, přehled z jednoho okna a integrovanou správu v celém podnikovém prostředí: pracovní stanice (fyzické i virtuální), servery a cloudové pracovní zátěže. GravityZone je cloudově orientované řešení, ale podporuje také nasazení v lokálních prostředích, pokud to vyžadují předpisy nebo obchodní požadavky.



Bitdefender GravityZone Ultra: Jednotná prevence, rozšířená detekce, reakce a analýza rizik

Bitdefender
GravityZone

eXtended Endpoint Detection and Response Business Security (XEDR)

Bitdefender v červenci 2021 dnes představil další evoluci řešení pro detekci a reakci na koncové body - eXtended EDR (XEDR) s přidáním analytiky a korelace bezpečnostních událostí napříč koncovými body do řešení Bitdefender Endpoint Detection and Response (EDR) a GravityZone Ultra, jednotné platformy pro prevenci, detekci a reakci na koncové body a analýzu rizik. Tyto nové funkce zvyšují účinnost zabezpečení pro identifikaci a zastavení šíření útoků ransomwaru, pokročilých trvalých hrozeb (APT) a dalších sofistikovaných útoků dříve, než ovlivní provoz podniku.

Díky integrované detekci a reakci napříč operačními systémy (Windows, Linux, Mac) a hybridními prostředími (veřejný a soukromý cloud, on-premises) poskytuje Bitdefender komplexní pohled na bezpečnostní operace v reálném čase, což výrazně zlepšuje schopnost organizací všech velikostí, dokonce i těch, které nemají bezpečnostní analytiky na plný úvazek, odhalovat skryté útoky, které by při izolované analýze a detekci na jednotlivých koncových bodech zůstaly nepovšimnuty.

Sofistikované útoky navržené tak, aby se vyhnuly detekci bezpečnostních technologií, často napodobují "normální" procesy nebo se provádějí ve více fázích prostřednictvím různých vektorů včetně koncových bodů, sítí, dodavatelských řetězců, hostovaných IT a cloudových služeb. Bitdefender XEDR zabraňuje komplexním útokům tím, že přijímá, zkoumá a koreluje telemetrii napříč koncovými body, aby odhalil indikátory kompromitace (IOC), techniky APT, signatury malwaru, zranitelnosti a abnormální chování. Toto pokročilé monitorování automatizuje včasnou detekci scénářů útoku a poskytuje pracovníkům zabezpečení a IT jednotný přehled o tom, kde útok začal.

Nové funkce XEDR také vylepšují řízenou detekci a reakci (MDR) Bitdefender tím, že poskytují větší přehled a kontext incidentu během vyšetřování, aby se urychlilo ověřování hrozeb, reakční akce a náprava.

Více informací o **EDR a jeho praktické použití** najdete ve dvoudílném videu na našem blogu

Bitdefender
GravityZone

Bitdefender Ransomware Mitigation

Ransomware je již dlouhou dobu lukrativním byznysem, který kyberzločincům vynáší miliardy na zaplacených výkupných. Nyní, když už je ziskovost ransomwaru prokázána, hledají zločinecké organizace nové a nové způsoby, jak na svých investicích ještě více vydělat, což povede k čím dál více sofistikovaným útokům na firmy a organizace.

Jak Bitdefender GravityZone poráží ransomware?
Jako adaptivní vrstvené bezpečnostní řešení poskytuje Bitdefender GravityZone několik funkcí proti ransomwaru, přičemž všechny jeho vrstvy spolupracují při prevenci, detekci a nápravě.

Více blokovacích vrstev	Koncový bod a síť, před provedením a při spuštění, na bázi souborů a bez souborů
Více detekčních vrstev	Kontrola procesů, monitorování registrů, kontrola kódu, hyperdetekce
Více vrstev obnovy	Účinný rollback z místního počítače, vzdáleného systému nebo bezpečnostního incidentu
Adaptivní obranné mechanismy	Pokročilý Anti-Exploit, adaptivní heuristika, konfigurovatelné strojové učení
Technologie pro minimalizaci rizik	Automatické opravování zranitelností, chybné konfigurace systému, chování uživatelů
Zálohy odolné proti neoprávněné manipulaci	Nepoužívá se zranitelná stínová kopie, ransomware nemůže odstranit zálohy.
Vzdálené blokování ransomwaru	Blokuje vzdálené a síťové útoky ransomwaru, a zařazuje IP adresy útočníků na černou listinu.
Čištění v rámci celé organizace	Vzdálené ukončování procesů, snadná globální karanténa a odstraňování souborů

Příklady použití **Případ použití Bitdefender Ransomware Mitigation** najdete ve videu na našem blogu.

Stáhněte si příručku „**Ransomware - Prevence a zmírnění škod pomocí Bitdefender GravityZone**“

Bitdefender
GravityZone

Sandbox Analyzer

Bitdefender Sandbox Analyzer je bezpečnostní řešení, které posiluje bezpečnostní infrastrukturu organizace proti sofistikovaným nebo cíleným útokům. Díky pokročilým detekčním a reportovacím schopnostem chrání před těžko zachytitelnými a přetrvávajícími hrozbami, které se snaží proniknout do vaší sítě.

Pokročilá detekce a viditelnost
Kombinuje vlastní toky zpravodajských informací o hrozbách s proprietárním strojovým učením a detekcí chování pro maximální přesnost v reálném čase. Zobrazuje interaktivní vizualizační grafy bezpečnostních incidentů pro hloubkovou forenzní analýzu. Detekuje velmi sofistikované, na míru vytvořené hrozby cílící na konkrétní prostředí pomocí golden image support.

Kompatibilní a efektivní
Prevence a detekce jsou prováděny plně na místě, bez souborů odeslaných pro skenování mimo vaši síť. Využívá AI a inteligenci hrozeb Bitdefender vytvořenou z více než 500 milionů uživatelů na celém světě, aby byla zachována přesná detekce v reálném čase na místní úrovni. Odhaluje nejpokročilejší typy malwaru, jako jsou APT nebo C2, a to prostřednictvím technologií anti-evasion a anti-fingerprint.

Integrovaný, automatizovaný, škálovatelný
Aby se prolínal s architekturou zabezpečení, integruje se nativně s technologiemi Bitdefenderu, a prostřednictvím API s dalšími prvky zabezpečení. Automatizuje proces výběru a odesílání souborů pro provedení karantény, a umožňuje autonomní reakci. Běží jako virtuální zařízení, může být snadno upraven tak, aby podporoval rostoucí toky dat.

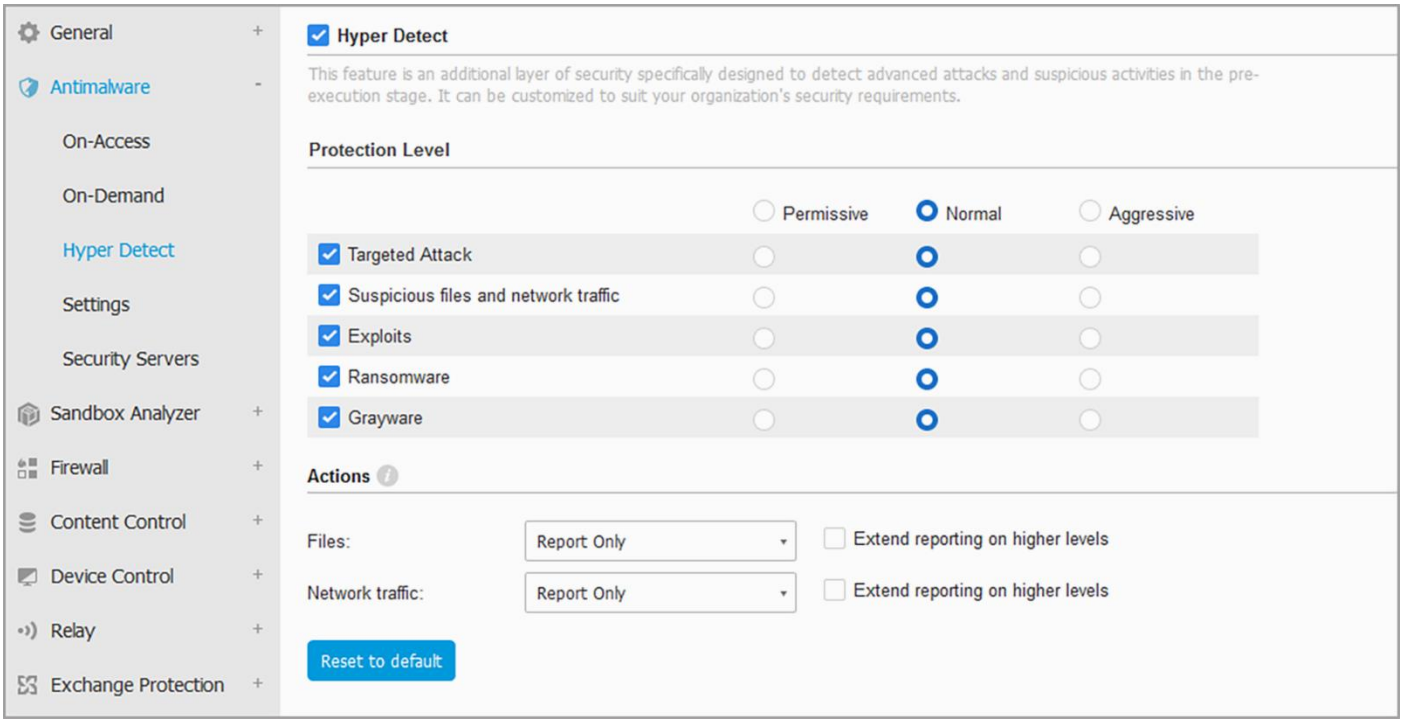
Více informací najdete na stránce produktu na našem webu Bitdefender.cz

Stáhněte si Datasheet „GravityZone™ Sandbox Analyzer“

HyperDetect

Tato obranná vrstva ve fázi před spuštěním obsahuje lokální modely strojového učení a pokročilé heuristiky vycvičené k odhalování hackerských útoků, nástrojů, exploitů a obfuskačních technik malwaru, aby bylo možné zablokovat sofistikované hrozby ještě před jejich spuštěním. Detekuje také způsoby šíření a stránky, které hostí sady zneužití, a blokuje podezřelý webový provoz.

HyperDetect umožňuje správcům zabezpečení upravit obranu tak, aby co nejlépe čelila konkrétním rizikům, kterým organizace pravděpodobně čelí. Díky funkci "pouze hlášení" mohou správci zabezpečení před zavedením nové obranné politiky připravit a sledovat její průběh, čímž se eliminuje přerušení provozu. V kombinaci vysoké viditelnosti a agresivního blokování, která je pro Bitdefender jedinečná, mohou uživatelé nastavit HyperDetect tak, aby blokoval na normální nebo povolené úrovni, a zároveň pokračovat v automatickém hlášení na agresivní úrovni, čímž odhalí včasné indikátory kompromitace.



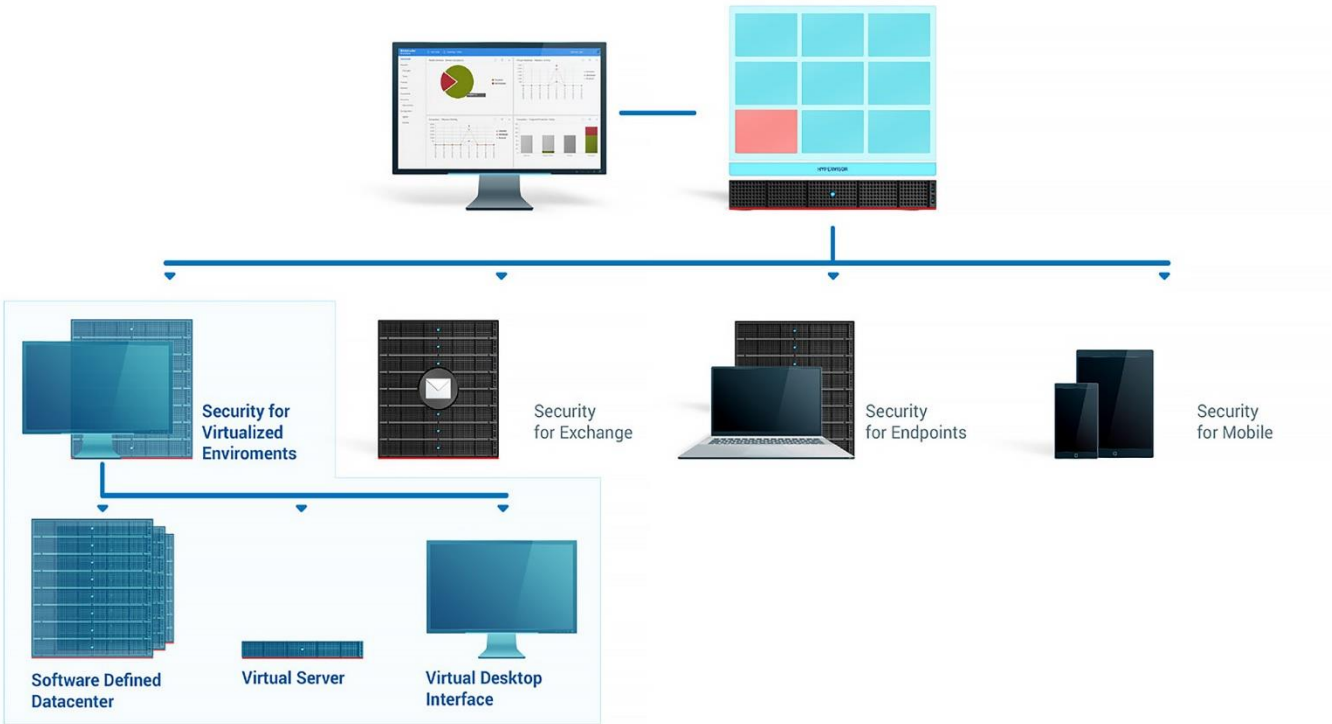
HyperDetect umožňuje správcům zabezpečení upravit agresivitu obrany a nabídnout možnost. jedinečnou kombinaci blokování a viditelnosti hrozeb. Například blokování na úrovni "Normální".a hlášení na úrovni "Agresivní".

GravityZone Security for Virtualized Environments

Vysoce výkonné zabezpečení pro hybridní a multicloudová prostředí
Bitdefender GravityZone Security for Virtualized Environments (SVE) je platformově orientované řešení ochrany navržené pro virtualizaci a hybridní cloud. Poskytuje osvědčené, vysoce výkonné zabezpečení v privátních i veřejných cloudových prostředích a přispívá k tomu, že společnost Bitdefender byla uznána jako lídr v nejnovější zprávě Forrester WaveTM: Cloud Workload Security, Q4 2019.

Podniky přijímají GravityZone SVE, aby minimalizovaly dopady na výkon zabezpečení cloudových výpočetních zdrojů a automatizovaly správu zabezpečení díky bezproblémové integraci s technologiemi VMware, Citrix, Nutanix a předními veřejnými cloudy, jako jsou Amazon a Azure.

Účelově vytvořený bezpečnostní zásobník cloudu a architektura s vysokou dostupností nabízejí robustní ochranu proti sofistikovaným útokům. GravityZone SVE konsoliduje správu zabezpečení nejen pro pracovní zátěže v hybridních a multicloudových prostředích, ale také pro fyzické desktopy, servery, mobilní zařízení a e-mail.



Bitdefender GravityZone (SVE) je nejpokročilejší bezpečnostní řešení pro virtualizovaná datová centra na trhu, pokud jde o antimalwarovou ochranu virtuálních počítačů, které optimalizuje nejen poměr konsolidace, ale také provozní náklady. GravityZone SVE je navrženo jako podnikové řešení schopné podporovat největší datová centra. Integrace do produkčního prostředí je však mimořádně jednoduchá a výhody technologie lze využít ve virtuálních prostředích libovolné velikosti.

GravityZone Email Security

Vícevrstvé cloudové zabezpečení e - mailů pro vaši organizaci a MSP.
S řešením GravityZone Email Security mohou organizace využívat kompletní ochranu podnikové elektronické pošty, která přesahuje rámec malwaru a dalších tradičních hrozeb, jako jsou spam, viry, rozsáhlé phishingové útoky a škodlivé adresy URL. Zabraňuje podvodům a vydávání se za někoho jiného, využívá několik předních bezpečnostních motorů a behaviorálních technologií k analýze obsahu příchozích a odchozích e-mailů, adres URL a příloh.

Vlastnosti & výhody

- **Více antivirových mechanismů založených na signaturách a chování** nabízí ochranu před všemi formami malwaru, včetně variant zero-day.
- **Ochrana při kliknutí** přepisuje adresy URL v e-mailových zprávách a chrání uživatele při kliknutí pomocí flexibilních zásad a stránek s upozorněním na blokování a varování.
- Možnost vynucení **šifrování TLS** a omezení komunikace s jinými e-mailovými servery, které nepodporují protokol TLS.
- **SecureMail** poskytuje jednoduché řešení šifrování e-mailů pro ochranu citlivých dat při přenosu.
- **Monitorování omezení odesílání** automaticky chrání před pokusy o odesílání velkého množství odchozích zpráv a pomáhá tak zabránit zařazení domény a IP na černou listinu.
- **Prevence Directory harvesting attack (DHA**) blokuje útoky directory harvesting tím, že uzavře spojení s příjemcem, jakmile je dosaženo prahové hodnoty neplatné / falešné e-mailové adresy.
- **Nearby (cousin) Domains** porovnává domény odesílatele s legitimními názvy domén a identifikuje blízké domény (které se od skutečného názvu domény liší o jeden nebo dva znaky).
- **Blokování příloh souborů** zahrnuje kontrolu MIME příloh a schopnost detekovat archivy chráněné heslem.
- **Opakované porovnávání vzorů**, algoritmická analýza, analýza na úrovni připojení a ověřování odesílatele/serveru, v kombinaci se zpravodajstvím o hrozbách, přináší další výkonnou vrstvu zabezpečení, která chrání uživatele služby Microsoft 365. Funkce **Executive Tracking** využívá údaje synchronizované ze služby Active Directory k automatickému zjišťování skutečných jmen uživatelů v polích záhlaví a obálek s adresami, aby byla zajištěna ochrana proti

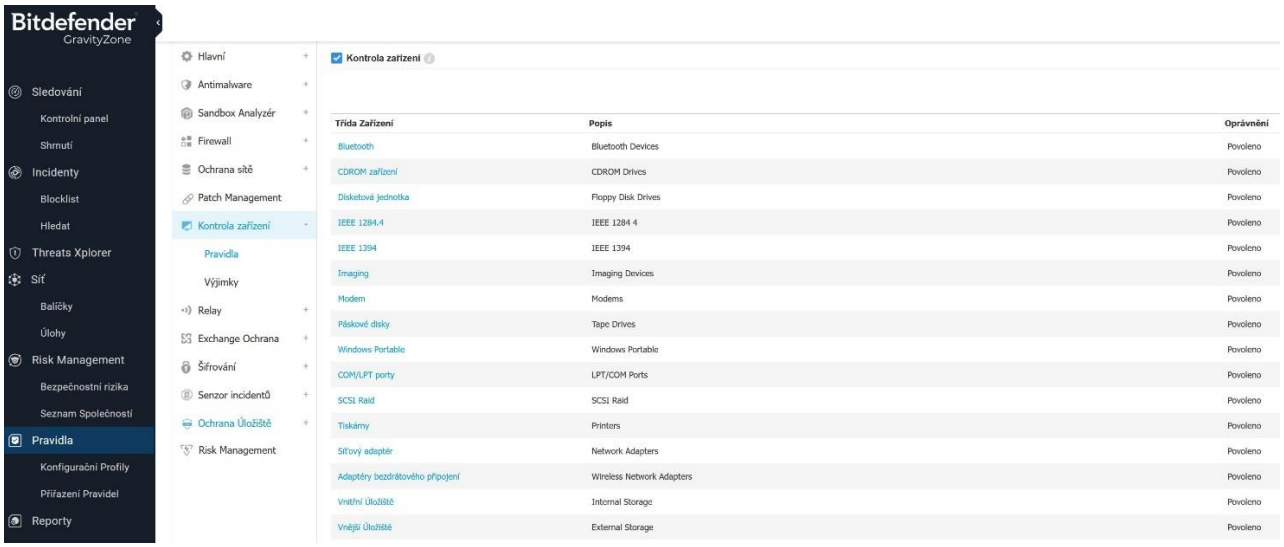
- **Podpora protokolů SPF, DKIM a DMARC**, které pomáhají chránit proti útokům typu "vydávání se za někoho jiného".
- útokům typu "vydávání se za jiné osoby" a CEO podvodům.

GravityZone Device Control

Vícevrstvé cloudové zabezpečení jednotlivých periférií pro vaši organizaci.
S řešením GravityZone ULTRA mohou organizace využívat kompletní ochranu podnikových zařízení. Modul Device Control umožňuje předcházet úniku citlivých dat a malwarovým infekcím prostřednictvím externích zařízení připojených ke koncovým bodům aplikací pravidel blokování a výjimek prostřednictvím zásad na širokou škálu typů zařízení..

Vlastnosti & výhody

- **Připojené zařízení ke spravovanému koncovému bodu** je reportováno do centrální konzole.
- **Škálovatelné** nastavení jednotlivých vlastností pro konkrétní skupiny či jednotlivce.
- Centrální vzdálená správa zařízení napříč sítí organizace i přes internet.
- **Detailní informace** včetně názvu zařízení, třídy, ID, data a času připojení.
- **Automatizace** přidělení jednotlivých profilů
- **Možnost nastavení výjimek** pro konkrétní zařízení.



Ukázka centrální konzole Device Management funkcionality přeložené do češtiny.

Bitdefender
GravityZone

Nabízíme Vám naprosto špičkové technologické řešení Bitdefender, které je dlouhodobě jedním z nejlepších na trhu což dokazují i nezávislé testy. Řešení Bitdefender pro vaš organizaci jde dál nad rámec požadovaného (EDR a Device Management), kdy v rámci jednoho řešení, jedné ceny, jednoho agenta centrální správy v kompletně lokalizovaném nástroji do českého jazyka pokryjete všechny potřebné oblasti.

- EDR – Endpoint Detection and Response – špičkové řešení se strojovým učením
- DEVICE CONTROL modul, plně integrovaný do platformy GravityZone, umožňuje organizacím kontrolovat jednotlivá připojovaná zařízení napříč prostředím i mimo něj
- EPP – Endpoint Protection Platform – zároveň kompletně vyřešíme bezpečnost koncového bodu nahrazením původního nástroje v rámci jednoho řešení.

KONTAKTNÍ INFORMACE

Bitdefender GOLD PARTNER

CYBOSEC s.r.o.
Bitdefender GOLD Partner

Hradčany 347, Smidary
Česká republika
tel.: [redacted]
email [redacted]

Technická podpora

tel.: [redacted]
email:
web: support.bitdef.cz

CYBOSEC We build the Trust

Bitdefender BUILT FOR RESILIENCE

KRYCÍ LIST NABÍDKY

Název zakázky

„Dodávka antivirového SW“.

Základní identifikační údaje o účastníkovi

Obchodní firma nebo název:	**CYBOSEC s.r.o.**
Sídlo / místo podnikání:	Hradčany 347, 503 53 Smidary
Právní forma:	Společnost s ručením omezeným
IČ:	04301226
DIČ:	CZ04301226
Spisová značka v obch. rejstříku:	C 42008
Osoba oprávněná jednat za účastníka:	Pavel Jícha, jednatel společnosti
Kontaktní osoba:	Pavel Jícha
Tel./Fax:	[redacted]
E-mail:	
Kritérium hodnocení:	**Nejnižší nabídková cena Kč bez DPH**

Cena bez DPH:	**419 622**	**Kč**
DPH:	88 120,62	**Kč**
Celková cena s DPH:	**507 742,62**	**Kč**

Podpisem tohoto krycího listu prohlašuji, že jsem byl důkladně seznámen se zadávací dokumentací vč. všech příloh, a že akceptuji veškeré podmínky.

V Praze dne 28.9.2022

Pavel Jícha, jednatel společnosti

……..

Jméno a podpis oprávněného zástupce účastníka

Bitdefender®
PARTNER ADVANTAGE PROGRAM

DIPLOMA

Bitdefender hereby certifies that

CYBOSEC s.r.o.

is qualified to attain GOLD Reseller status

[redacted]
Bogdan Irina

GOLD
Reseller

NABÍDKA

NAB-22-277
Vystaveno: 28.9.2022

Dodavatel:
CYBOSEC s.r.o.
Hradčany 347
503 53 Smidary
Česká republika

IČO: 04301226
DIČ: 04301226

Kontaktní údaje:

Pavel Jícha
[redacted]

Odběratel:
Město Sokolov

IČO: 00259586
DIČ: CZ00259586

Rokycanova 1929
35601 Sokolov
Česká republika

Kontaktní údaje:

Položka	Množství	Cena za jednotku	Sleva %	Celkem	Sazba DPH	Celkem vč. DPH
Bitdefender GravityZone Business Security ENTERPRISE - GOV 36 měsíců	300	1 396,00 Kč	0	418 800,00 Kč	21 %	506 748,00 Kč
Instalace nástroje (senior technik)	3	15 000,00 Kč	99	450,00 Kč	21 %	544,50 Kč
Certifikované zaškolení obsluhy (BASIC ADMIN / vzdáleně)	1	15 000,00 Kč	99	150,00 Kč	21 %	181,50 Kč
Konzultace 4hod pro 1.rok	4	1 850,00 Kč	99	74,00 Kč	21 %	89,54 Kč
Konzultace 4hod pro 2.rok	4	1 850,00 Kč	99	74,00 Kč	21 %	89,54 Kč
Konzultace 4hod pro 3.rok	4	1 850,00 Kč	99	74,00 Kč	21 %	89,54 Kč

Rozpis DPH

Sazba %	Základ	Daň
21%	419 622,00 Kč	88 120,62 Kč

Konečná cena: **419 622,00 Kč**
Konečná cena vč. DPH: **507 742,62 Kč**